Audit Report

YEAR 2000 STATUS OF THE ARMY
TOTAL ASSET VISIBILITY SYSTEM

Report No. 99-172 May 28, 1999

Office of the Inspector General
Department of Defense

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Year 2000 Status of the Army Total Asset Visibility System

B. DATE Report Downloaded From the Internet: 08/09/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 08/09/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900 The identity of each writer and caller is fully protected.

Acronyms

A-TAV	Army Total Asset Visibility
LOGSA	Logistics Support Activity
Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

May 28, 1999

MEMORANDUM FOR DEPUTY UNDER SECRETARY OF DEFENSE
(LOGISTICS)
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Year 2000 Status of the Army Total Asset Visibility System (Report No. 99-172)

We are providing this report for your review and comment. We performed this audit in response to a congressional request. We considered management comments of the Army on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly The Army comments were only partially responsive. Therefore, we request additional comments on Recommendations 1.a (1), (2), and (3); 1.b; 1.c.; and 2.a. Also as a result of management comments we added Recommendation 2.b. to the Army and Recommendations 3.a. and 3.b. to the Director, Logistics Systems Modernization. We request that the Army and the Director, Logistics Systems Modernization, provide comments by June 9, 1999.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. George Cherry at (703) 604-9018 (DSN 664-9018) (email hgcherry@dodig.osd.mil), Ms. Kathryn M. Truex at (703) 604-9045 (DSN 664-9045) (email kmtruex@dodig.osd.mil), or Ms. Mary Lu Ugone at (703) 604-9049 (DSN 664-9049) (email mlugone@dodig.osd.mil). See Appendix B for the report distribution. The audit team members are listed inside the back cover

Robert J. Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-172 **May 28, 1999**
(Project No 9AS-0090)

Year 2000 Status of the Army Total Asset Visibility System

Executive Summary

Introduction. This report is one in a series being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a listing of audit projects addressing the issue, see the year 2000 webpage on the IGnet at http://www.ignet.gov.

The National Defense Authorization Act for 1999 requires "the DoD Inspector General to selectively audit information technology and national security systems certified as year 2000 compliant to evaluate the ability of systems to successfully operate during the actual year 2000 to include their ability to access and transmit information from point of origin to point of termination."

The Army Total Asset Visibility is a mission-critical Army system that provides managers and decisionmakers at various echelons and within various user communities with a single authoritative source of asset and force information.

Objectives. The overall audit objective was to evaluate the ability of the Army Total Asset Visibility system to operate successfully in the year 2000, including the system's ability to access and transmit information from point of origin to point of termination. Additionally, the audit determined whether an adequate contingency plan existed to ensure continuity of operations and whether the system status reporting has been accurate.

Results. The Army Total Asset Visibility system was prematurely certified as year 2000 compliant. The certification was premature because the system was tested in a noncompliant operating environment and did not go through interface testing. Additionally, the Army Total Asset Visibility system contingency plan was incomplete and had not been fully distributed to and coordinated with the functional users As a result, the Army Total Asset Visibility system remains at risk of failure.

Summary of Recommendations. We recommend that the Army recertify the Army Total Asset Visibility system and support the recertification with documentation of system interface testing, with test plans and test results, dated and signed by the appropriate testing officials, and a completed certification checklist, which notes the results of external interface testing completed. If recertification is not complete before

the next quarterly report to the Office of the Secretary of Defense, we recommend that the Army adjust the Office of Secretary of Defense year 2000 database and corresponding report to the Office of Management and Budget to indicate that the Army Total Asset Visibility system has not yet been certified as year 2000 compliant. We also recommend that the Army alert the Director, Logistics Systems Modernization that the Army Total Asset Visibility system has not completed systems certification testing requirements. Additionally, we recommend that the Director, Logistics Systems Modernization use the A-TAV contingency procedures in the Logistics End-to-End Test, instead of the A-TAV system; and require that the Army test the A-TAV contingency procedures before using them in the Logistics End-to-End Test. The Army Total Asset Visibility contingency plan also requires more detailed basic interface descriptions; the identification of plan trigger dates, activities, strategies, and procedures to be performed; a detailed description of manual procedures; and a discussion of the acceptable level of performance and the risk arising from the use of manual procedures. The contingency plan should be coordinated with and distributed to the functional users and others involved with making the plan work. For details of the audit results, see the Finding section of the report.

Management Comments. The Office of the Secretary of the Army nonconcurred with our recommendation to recertify the Army Total Asset Visibility system and to include in the recertification a discussion of completed interface testing, official test plan and test results, and completion of the certification checklist that would note the results of external interface testing. The Army stated that interface testing was not required because no format changes had been made to Army Total Asset Visibility system interfaces. Additionally, the Army Total Asset Visibility system will participate in the Army End-to-End Test that began May 6, 1999,[1] and that it would be impractical to require the Army to recertify and would deny Army Total Asset Visibility system participation in the Office of the Secretary of Defense sponsored end-to-end logistics tests that started May 25, 1999 [and will end July 23, 1999]. Additionally, the Army stated that a third party contractor completed an Independent Verification and Validation process for the Army Total Asset Visibility system and found the system to be certified. The Army further stated that to start the certification process again would cost an additional $34,148, which the Army did not consider a prudent expenditure of Army dollars. The Army concurred with the recommendations covering improvements to and coordination of the Army Total Asset Visibility system contingency plan. A discussion of the management comments is in the Findings section of the report and the complete text is in the Management Comments section.

Audit Response. The Army's comments on recertifying the Army Total Asset Visibility system are nonresponsive. Contrary to the Army stated position, the DoD Management Plan requires interface testing before certification. The Army comments appear to indicate that it plans to rely upon the end-to-end tests to provide assurance that the Army Total Asset Visibility system interfaces are appropriately tested. We do

[1] On May 20, 1999, at the Test Readiness Review for the Logistics End-to-End Testing, the Army Total Asset Visibility system was reported as being unable to operate on the time machine for the Army Logistics End-to-End test.

not agree that end-to-end test events should be used in lieu of required system certification testing requirements. The test events lack the rigor of certification testing and do not provide the same level of assurance as proper system certification tests. Additionally, it still is unclear what mainframe operating environment the Army used to certify Army Total Asset Visibility system as year 2000 compliant. We request the Army to reconsider its position and provide comments to the final report. We added a recommendation for the Army to notify the Director, Logistics Systems Modernization, that the Army Total Asset Visibility system did not adequately complete systems certification testing requirements. Also, we added a recommendation that the Director, Logistics Systems Modernization use the A-TAV contingency procedures in the Logistics End-to-End Test, instead of the A-TAV system; and require that the Army test the A-TAV contingency procedures before using them in the Logistics End-to-End Test. We have requested that the Army and the Director, Logistics Systems Modernization provide comments on the final report by June 9, 1999.

Table of Contents

Introduction

The National Defense Authorization Act for FY 1999 requires the Inspector General, DoD, to selectively audit information technology and national security systems certified as year 2000 (Y2K) compliant to evaluate the ability of systems to successfully operate during the actual year 2000, including their ability to access and transmit information from point of origin to point of termination.

Background

DoD Year 2000 Management Strategy. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), in his role as the DoD Chief Information Officer, issued the "DoD Year 2000 Management Plan," Version 2.0 (DoD Management Plan), in December 1998. The DoD Management Plan provides the overall DoD strategy and guidance for fixing, testing, and implementing compliant systems and monitoring progress. The DoD Management Plan describes in detail what each DoD Component must accomplish in each phase of the required five-phase Y2K management process. The target completion date for implementing all mission-critical systems was December 31, 1998. Appendix I of the DoD Management Plan provides guidance on planning, executing, and evaluating activities required to assess Y2K readiness.

Army Total Asset Visibility. The Army Total Asset Visibility system (A-TAV) is a mission-critical Army system that provides managers and decisionmakers at various echelons and within various user communities with a single authoritative source of asset and force information. The A-TAV system assimilates data from as many as 42 data sources or resident databases on requirements and authorizations; force structure; weapons systems configuration; and assets in use, in supply, in process, or in transit, as well as other miscellaneous item data. Accordingly, the A-TAV is dependent upon other systems to be able to perform its functions. The Army Logistics Support Activity (LOGSA), a subordinate organization of the Army Materiel Command, is the program manager for the A-TAV system.

Operational Environment. The A-TAV runs on two Amdahl mainframe computers currently located at the Defense Megacenter in Huntsville, Alabama. Users of the system can access A-TAV data stored on the mainframe through graphical user interfaces. Other users prefer to access A-TAV data stored in two LOGSA-owned servers. A-TAV also receives a small portion of its data from suppliers who log in and send data to a server.

Reported Year 2000 Status. The Commanding Officer for the LOGSA certified the system as Y2K compliant on December 22, 1998. A-TAV appeared in the DoD Y2K database, effective December 31, 1998, as certified

and in the implementation phase. A-TAV is scheduled for further Y2K compliance testing in the Army and DoD logistics end-to-end tests from April 13, 1999 through August 20, 1999.

Objectives

The overall audit objective was to evaluate the ability of the A-TAV to operate successfully in the year 2000, including the system's ability to access and transmit information from point of origin to point of termination. Additionally, the audit determined whether an adequate contingency plan existed to ensure continuity of operations and whether the system status reporting has been accurate. See Appendix A for a discussion of the audit scope and methodology.

Year 2000 Status of the Army Total Asset Visibility System

The LOGSA should not have certified A-TAV as Y2K compliant as of December 1998. The A-TAV should not have been certified because supporting test plans and test results showed that LOGSA had tested A-TAV in a noncompliant operating environment and had not performed interface testing. Additionally, the A-TAV contingency plan did not adequately provide an overview of the system requirements or discuss the use of manual procedures or testing of the contingency plan itself. Also, LOGSA did not fully distribute and coordinate the contingency plan with the functional users. As a result, without a rigorous system testing and certification process, and a comprehensive contingency plan, the functionality provided by A-TAV remains at risk of failure.

Certification

The DoD Management Plan, Section A.4.5, requires that system developers, maintainers, and the functional proponent certify and document each system's Y2K compliance. Compliance should be certified in accordance with the Y2K compliance checklist provided in Appendix G of the DoD Management Plan.

Section A.4.5 further states the following:

> A signature by the System Manager, the Project Manager, and the customer on the checklist confirms that testing was completed in accordance with the Management Plan and the results indicated that the system is Y2K compliant.

A-TAV Certification. The LOGSA should not have certified A-TAV as Y2K compliant because the critical requirements for certification had not been met as of December 1998. The LOGSA provided us a test plan, "Army Total Asset Visibility (A-TAV) Year 2000 Compliance Software Test Plan," Version 1.1, undated and unsigned, and results, "Army Total Asset Visibility (A-TAV) Year 2000 Compliance Software Test Report," Version 1.1., undated and unsigned, as the basis for supporting the A-TAV certification. However, the test plan and test results showed that the system was tested in a noncompliant operating environment and that critical interfaces had not been certified and tested with A-TAV.

Operating Environment

A-TAV runs on two mainframe computers in the Huntsville, Alabama, Defense Megacenter. Additionally, A-TAV uses two LOGSA owned servers and assorted personal computers to store, process, and access data. A-TAV customers worldwide may use their own personal computers to access A-TAV data stored either on the mainframe or on the server.

Compliant Operating Environment. The DoD Management Plan Appendix A.4.6 requires that "all systems must be tested on a compliant domain and in an operationally compliant environment" before system certification. Neither the Defense Information Systems Agency owned mainframes nor the LOGSA owned servers provided a fully compliant operating environment for testing and certification of A-TAV.

Defense Information Systems Agency Owned Mainframes. The LOGSA tested A-TAV for Y2K compliance in the same environment in which the application runs, in its production mode, on two mainframes in the Huntsville, Alabama, Defense Megacenter. During system testing, the operating environment on those two mainframes contained at least 20 noncompliant software products.

The "Army Total Asset Visibility (A-TAV) Year 2000 Compliance Software Test Plan," Version 1.1, Section 3.1.1.1, lists specific mainframe software products as necessary to perform Y2K testing. The following table compares the products that LOGSA identified as necessary for testing with what was installed on the mainframes where testing was performed.

Comparison of A-TAV Test Plan Requirements to Defense Megacenter Operating Environment

Item	A-TAV Test Plan Requirement	Defense Megacenter Installed Product	Defense Megacenter Version Y2K Compliant
Operating System	OS/390, Version 1, Release 3	OS/390, Version 1, Release 2	Yes
Compilers	Model 204, Version 4.1.01	Model 204, Version 4.1	Yes
Communication Software	KNET TCP/IP, Release 6.0	KNET TCP/IP, Release 5.0	No
Related Application Software	CICS, Version 2.1.2	CICS, Version 2.1.2	No
Databases	DC/DB, Version 8.1	DC/DB, Version 8.1	No

OS	Operating System
TCP/IP	Transmission Control Protocols and Internet Protocols
CICS	Customer Information Control System
DC/DB	Datacom Database

According to the test plan and results that LOGSA provided, A-TAV testing was performed not only using non Y2K-compliant versions of the products, but also using down-level versions of software required by the test plan.

The LOGSA Commander explained that he had certified A-TAV based upon what he considered to be his organization's responsibilities and disregarded those aspects of the system outside of his immediate control. Because the Defense Information Systems Agency is responsible for making its own hardware and executive software Y2K compliant, the LOGSA Commander stated that he was unwilling to hold up the certification of A-TAV and any other LOGSA systems. He added that LOGSA had proceeded in accordance with Army direction.

LOGSA Owned Servers. A-TAV also uses two LOGSA owned servers to process and store A-TAV data. Neither of the two LOGSA servers used to support A-TAV were fully Y2K compliant at the time of A-TAV certification.

The DoD Management Plan Appendix A.4.1 strongly suggests that DoD Components test all commercial off-the-shelf and Government off-the-shelf products for Y2K compliance. The DoD Management Plan further states that testing, as a minimum, assumes that all commercial off-the-shelf and Government off-the-shelf products, including operating systems, and third-party software are considered Y2K compliant by their vendors.

We looked for evidence of vendor certifications or testing to support the Y2K compliance for the hardware and associated software on the servers. The results follow.

Hardware and Operating Software. The 2 servers consist of a total of 15 hardware and operating software commercial off-the-shelf products. Eight of those products were either compliant without a patch or had been patched to make them Y2K compliant. However, the remaining seven products either needed patching or were scheduled to be removed and replaced with Y2K-compliant versions of the product.

Security Software. Additionally, the Sun server uses two DoD-mandated security packages for which LOGSA could not provide documentation to support Y2K compliance.

The LOGSA considered servers not to be A-TAV system components, but to be infrastructure. Therefore, the servers were not included in the A-TAV testing plans and certification. However, the LOGSA functional user representatives considered the servers to be part of the A-TAV system.

Updated Status. On March 22, 1999, we met with Army representatives to discuss the results of this audit. Representatives from the Army Materiel Command provided another copy of the "Army Total Asset Visibility (A-TAV) Year 2000 Compliance Software Test Plan," Version 1.1, undated and unsigned, and of the Software Test Report, Version 1.1., undated and unsigned. The Army Materiel Command copies of the test plan and test report, although both were marked version 1.1, no longer referenced the noncompliant mainframe products that were identified as required in the LOGSA-provided test plan and results. Accordingly, we could not tell which copies of the test plan and test reports are correct with respect to mainframe compliance.

Additionally, neither version addressed the testing of the LOGSA servers. However, since the completion of audit fieldwork and in response to the discussion draft for this report, LOGSA states that it had installed all updates required to make the servers at LOGSA Y2K compliant. LOGSA should recertify A-TAV to authenticate the original A-TAV certification.

Interfaces

Automated information technology processes that deal with year-date functions face the risk of failure before, on, and after January 1, 2000. The problem becomes increasingly complex because corrupted data can be perpetuated through interfaces with other information systems. The average system, for example, is connected to a number of other feeder systems. All of the systems and their interfaces must perform correctly to ensure Y2K functionality.

Guidance. Before system managers report a system as exiting from the Y2K validation phase, the DoD Management Plan Section A.4.6 requires all system interfaces to have been tested and certified as Y2K compliant.

Additionally, Appendix G of the DoD Management Plan provides the Y2K compliance checklist for certification. The checklist should be completed before certification of the system and the responses considered in whether the system is actually ready to be certified. Question G.6 of the Y2K certification checklist asks whether "external interfaces have been identified and validated to correctly function for all dates." The interaction between a system and any other external data source, if existing, must be verified for correct operation.

Interface Status. The A-TAV system interfaces with approximately 50 other external and internal systems. However, neither version of the A-TAV test plan nor the A-TAV test results address interface testing. The LOGSA testers responded on the certification checklist that question G.6 was "not applicable" to A-TAV, and the LOGSA commander certified the system without further addressing the issue of interfaces. LOGSA also reported A-TAV in the DoD Y2K database as having exited from the validation phase on December 22, 1998. Documentation supporting the certification checklist should include the results of interface testing.

Contingency Plan

Purpose. Contingency plans provide insurance against the many possible types of Y2K disruptions. They help expedite the restoration of the system to continue the mission or function while system support is not available, regardless of the reason for the disruption.

Guidance. The DoD Management Plan requires both a system contingency plan and an operational contingency plan for all nondevelopmental mission-critical systems. The system contingency plan focuses on the restoration of a system thought to be Y2K compliant. The system contingency plans should have been finalized and distributed no later than December 30, 1998. The operational contingency plan focuses on how to complete the mission or function without the support of any or all mission-critical support systems.

Both system and operational contingency plans are highly interrelated. The system contingency plan must track to at least one operational contingency plan to ensure that an alternative system or procedure is available in the event that the system experiences a Y2K disruption. To facilitate coordination of the operational and system requirements, the DoD Management Plan also requires contingency plans started in the assessment phase to be updated throughout the Y2K resolution process. Appendix H.1 of the DoD Management Plan specifically requires the following:

> Personnel should be trained in the execution of contingency plans and the plans should be tested and updated periodically to assure that they remain current and valid. Relevant contingency information should be exchanged between program/system managers of interfaced systems and with all system users.

A-TAV Contingency Plan. The LOGSA initially provided us with a draft contingency plan for A-TAV, version 1.0, dated January 26, 1999. On March 22, 1999, we met with Army representatives to discuss the results of this audit. At that time, representatives from the Army Materiel Command provided an updated copy of the A-TAV contingency plan, also identified as version 1.0, but dated March 16, 1999. Both contingency plans state that they address programmatic risk management and operational failure and recovery.

The A-TAV contingency plan did not discuss strategies and trigger dates, the use of manual procedures, or testing of the contingency plan itself. Additionally, the plan had not been signed, nor had it been distributed to or coordinated with program or system managers of interfacing systems and with all system users as required.

Overview. The January 26, 1999, A-TAV contingency plan did not adequately cover the system mission or address A-TAV core processes. The contingency plan did delegate to the Y2K program manager authority to invoke the plan and execute the procedures in the plan. However, the plan did not explain the roles and responsibilities of the other essential personnel. Although the plan did include interface points of contact, it did not provide a basic description of interfaces. The contingency plan also failed to address contingency plan trigger dates, activities, strategies, and procedures to be performed at the exact time when the date becomes January 1, 2000. The March 16, 1999, contingency plan did add a brief description of the system mission, but the other deficiencies remain.

Back-up Plan. In the January 26, 1999, A-TAV contingency plan, LOGSA did address A-TAV back-up procedures under emergency contingency operations and interim contingency operations; however, the specific guidelines given in the back-up plans were incomplete. The plan failed to identify responsible personnel and did not address additional staffing requirements, hardware and software requirements, or workarounds. The March 16, 1999, contingency plan did assign responsibilities to specific managers, address additional resource requirements, and add details on workarounds. Therefore, this report contains no recommendations to further modify the back-up plan in the contingency plan

Use of Manual Procedures. The January 26, 1999, A-TAV contingency plan did not identify manual procedures as part of the contingency plan. The March 16, 1999, contingency plan did briefly mention the use of manual procedures, but it did not describe the manual procedures in detail.

Testing the Contingency Plan. Neither contingency plan addressed when, where, and the manner in which the contingency plan would be tested.

Coordination. Neither plan had been distributed to major functional users or owners of A-TAV.

Summary

The LOGSA should not have certified the A-TAV system as Y2K compliant as of December 1998 because A-TAV did not meet critical requirements for certification. LOGSA provided a test plan and test results that showed that A-TAV was tested in a noncompliant operating environment and that testing of interfaces was not done. Undated and unsigned versions of supporting test plans and test results contradict one another on the executive software that should have been used to test the A-TAV system in a mainframe environment. Further, the LOGSA owned servers used for A-TAV had not been made Y2K compliant at the time of certification. Additionally, the A-TAV contingency plan was incomplete and had not been fully distributed and coordinated. Accordingly, we believe that the functionality provided by A-TAV remains at risk of failure.

Recommendations, Management Comments, and Audit Response

Added and Renumbered Recommendations. As a result of management comments and additional information, we added three new recommendations. We renumbered Recommendation 2 to be 2.a. We added Recommendation 2.b., which requires the Army Chief Information Officer to notify the Director, Logistics Systems Modernization that the A-TAV did not complete systems certification testing requirements. We also added Recommendations 3.a. and 3.b., requiring that the Director, Logistics Systems Modernization, use the A-TAV contingency procedures in the Logistics End-to-End Test, instead of the A-TAV system and that the Army test the A-TAV contingency procedures before using them in the Logistics End-to-End Test;

1. We recommend that the Commander, Army Logistics Support Activity:

a. Recertify the Army Total Asset Visibility system with the following changes:

(1) Discuss the interface testing completed;

(2) Require a supporting test plan and results that are dated and signed by the testing official; and

(3) Complete the certification checklist and note the results of external interface testing completed, rather than responding "not applicable."

Army Comments. The Army nonconcurred with our recommendation to recertify the A-TAV and to include in the recertification a discussion of completed interface testing, official test plan and test results, and completion of the certification checklist that would note the results of external interface testing. The Army stated that interface testing was not required because no format changes were made to A-TAV interfaces. Additionally, the A-TAV will participate in the Army end-to-end test beginning May 6, 1999[2], and that to require the Army to recertify would be impractical and would deny A-TAV participation on the Office of the Secretary of Defense sponsored end-to-end logistics tests that started on May 25, 1999 [and will end on July 23, 1999]. Additionally, the Army stated that a third party contractor completed an Independent Verification and Validation process for A-TAV and found A-TAV to be certified. The Army further stated that to start the certification process again would cost an additional $34,148, which the Army did not consider a prudent expenditure of Army dollars.

Audit Response. We consider the Army comments to be nonresponsive. The Army comments amplify our concerns regarding the rigor of the A-TAV certification testing and as to whether the A-TAV certification can be prudently used as a measure of assurance in Y2K operational readiness. Contrary to the Army stated position, the DoD Management Plan does not remove the requirement for testing even if a system does not have interface format changes. The change in the DoD Management Plan cited by the Army clarifies guidance on testing and certification of interfaces, but does not support the position that interface testing is not required for certification. Based on the clarified guidance, if the A-TAV did not have format changes, system interfaces would require testing independently by the system developer, but not joint testing with interface partners.

It is well understood that when the format of a system is changed, all of the data that follows the modification in the interface may be affected. Therefore, joint changes and testing is required. When the format is unaffected and interface dates continue to use two character years, then the year 2000 and beyond must be interpreted using an agreed upon rule. This is a logical interface change and the receiver's date interpretation rule must match the provider's date interpretation rule for the interface to communicate properly. Therefore, evidence that the receiver implemented and tested the provider's documented rule is necessary to minimize the risk of corrupted data in the receiver's system. The Army's comments incorrectly assert that such interface testing to an agreed

[2] On May 20, 1999, at the Test Readiness Review for the Logistics End-to-End Testing, the A-TAV was reported as being unable to operate on the time machine for the Army Logistics End-to-End test

upon rule is not required. The DoD Management Plan requires interface testing, and in this instance, interface testing to an agreed upon rule (spelled out in the interface agreements).

The independent verification and validation process mentioned in the Army comments also apparently did not include the required interface testing because the test plan and results did not discuss interface testing and the certification checklist indicated that interface testing was not applicable. To compound matters, it was unclear as to what mainframe operating environment was used to certify A-TAV as Y2K compliant.

Further, the Army comments appear to indicate that it plans to rely upon the end-to-end tests to provide assurance that A-TAV interfaces are appropriately tested. We do not agree that end-to-end test events should be used in lieu of required system testing and certification requirements. The test events do not provide the same level of assurance as proper system certification tests. Primary Y2K assurance comes from properly conducted system certification tests, which test all interfaces, all system subcomponents, and all hardware and software used by an application in an operational environment. End-to-end test events are limited to exercising a fewer number of interfaces, system subcomponents, and dates; and lack the rigor of certification testing.

Finally, the fact that A-TAV needs to be certified before it could participate in the Office of the Secretary of Defense sponsored logistics end-to-end tests should highlight the importance of proper certification. The Army should use the contingency procedures for A-TAV in the Logistics End-to-End Test because A-TAV was not properly certified.

We have asked the Army to reconsider its position on Recommendations 1.a (1), (2), and (3).

b. Write a contingency plan, to be signed and dated by a responsible official, that includes:

- **a description of the basic interfaces;**
- **identification of contingency plan trigger dates, activities, strategies, and procedures to be performed at specified dates or events;**
- **a detailed description of manual procedures to be performed;**
- **a discussion of the acceptable level of performance and the risk arising from the use of manual procedures; and**
- **a plan to test the contingency plan itself.**

Army Comment. The Army concurred with Recommendation 1.b. stating that version 1.0 of the A-TAV contingency plan dated April 16, 1999, does provide a description of interfaces, contingency plan trigger dates, strategies and

procedures to be performed at specific dates as well as manual procedures and work arounds. Information on an acceptable level of risk will be added to the A-TAV contingency plan no later that June 1, 1999. Additionally, the contingency plan will be exercised prior to June 30, 1999. in accordance with the requirement of the DoD Management Plan.

Audit Response. The Army comments are partially responsive. The revised version of the A-TAV contingency plan, version 1.0, dated April 16, 1999, adequately identifies contingency plan trigger dates and provides strategies and procedures to be performed at specific dates. However, we still believe that acronym listings without definition and purpose are not sufficiently descriptive of the A-TAV interfaces. Furthermore, manual procedures or any other procedures required, even if they consist of reliance on the continuity of operations plan, should be included or referenced in the A-TAV Y2K contingency plan. Accordingly, we have asked the Army to reconsider its position on these sections of Recommendation 1.b. and provide comments on the final report.

c. Coordinate the contingency plan with the functional users and all involved with making the plan work and distribute copies of the plan to all interested parties.

Army Comment. The Army concurred with Recommendation 1.c. stating that the contingency plan has been coordinated with the functional users and all involved with making the plan work. Copies of the plan will be distributed to all interested parties no later than July 30, 1999.

2. We recommend that the Army Chief Information Officer:

a. Adjust the Office of the Secretary of Defense year 2000 database and report to the Office of Management and Budget that the Army Total Asset Visibility system is in the validation phase and not certified as year 2000 compliant, if recertification of the Army Total Asset Visibility system is not complete before the next quarterly status report to the Office of the Secretary of Defense.

Army Comments. The Office of the Secretary of the Army nonconcurred with our recommendation to report A-TAV as not year 2000 certified in the Secretary of Defense year 2000 database or to the Office of Management and Budget. The Office of the Secretary of the Army considers A-TAV to have been adequately certified as year 2000 compliant

Audit Response. We consider the Army comments to be nonresponsive. The Army has not satisfied the DoD Management Plan requirements for system certification. Therefore, the Army should report A-TAV as not year 2000 certified in the Office of the Secretary of Defense year 2000 database and to the Office of Management and Budget. We ask that the Army reconsider its position and provide comments on the final report.

b. Notify the Director, Logistics Systems Modernization that the A-TAV did not complete systems certification testing requirements.

3. We recommend that the Director, Logistics Systems Modernization:

a. Use the A-TAV contingency procedures in the Logistics End-to-End Test, instead of the A-TAV system; and

b. Require that the Army test the A-TAV contingency procedures before using them in the Logistics End-to-End Test.

Appendix A. Audit Process

This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a listing of audit projects addressing the issue, see the Y2K web page on the IGnet at http://www.ignet.gov.

Scope

We judgmentally selected A-TAV from those mission-critical information systems reported in the DoD Y2K database as of December 31, 1998. We met with Army and Defense Information Systems Agency management and technical personnel to discuss their efforts in resolving the Y2K computing issues on the A-TAV system. We also reviewed A-TAV system inventories, test plans, test results, certification documents, and contingency plans to evaluate the risk of the A-TAV system successfully operating in the year 2000. We compared the LOGSA efforts in working the A-TAV Y2K issues with those requirements described in the DoD Management Plan that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) published in December 1998 and the Army Action Plan published in June 1998.

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Department of Defense has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objectives and goals.

> **Objective:** Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. **(DoD-3)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals.

- **Information Technology Management Functional Area.**

  Objective: Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM-1.2)**

- **Information Technology Management Functional Area.**

  Objective: Provide services that satisfy customer information needs. **Goal:** Modernize and integrate Defense information infrastructure. **(ITM-2.2)**

- **Information Technology Management Functional Area.**

  Objective: Provide services that satisfy customer information needs.
  Goal: Upgrade technology base. **(ITM-2.3)**

General Accounting Office High-Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risk in resolution of the Y2K problem as high. This report provides coverage of that problem and of the overall Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit at LOGSA from February through May 1999, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data for this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance.

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil.

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Deputy Under Secretary of Defense, Logistics
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)*
  Principal Director for the Year 2000*
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Chief Information Officer, Army
Inspector General, Department of the Army
Commander, Army Materiel Command
  Commander, Logistics Support Activity
Auditor General, Department of the Army*

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Chief Information Officer, Navy
Inspector General, Department of the Navy
Auditor General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Air Force
Inspector General, Department of the Air Force
Auditor General, Department of the Air Force

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Chief Information Officer, General Services Administration
Office of Management and Budget
  Office of Information and Regulatory Affairs
General Accounting Office
  National Security and International Affairs Division
    Technical Information Center
Director, Defense Information and Financial Management Systems, Accounting and Information Management Division, General Accounting Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Special Committee on the Year 2000 Technology Problem
Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Department of the Army Comments

Final Report Reference

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Director of Information Systems for Command, Control Communications, & Computers

13 MAY 1999

SAIS-IIAC

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, 400 ARMY NAVY DRIVE, ARLINGTON, VA 22202

SUBJECT: Audit report on Year 2000 Status of the Army Total Asset Visibility System (Project No 9AS-0090)

Reference DODIG Memorandum, April 20, 1999, subject as above The Army Materiel Command's response to recommendation 1 is attached. The response to recommendation 2 is as follows:

Recommendation 2: We recommend that the Army Chief Information Officer adjust the Office of the Secretary of Defense year 2000 database and report to the Office of Management and Budget that the Army Total Asset Visibility system is in the validation phase and not certified as year 2000 compliant, if recertification of the Army Total Asset Visibility system is not complete before the next quarterly status report to the Office of the Secretary of Defense.

Renumbered as Recommendation 2 a

Response: Nonconcur. For the reasons provided in the attached memorandum, the Army Total Asset Visibility system has been certified as year 2000 compliant in accordance with the Department of Defense Year 2000 Management Plan The Army input to the Department of Defense year 2000 database and the quarterly report to the Office of Management and Budget does not need to be changed to reflect a different status for the Army Total Asset Visibility system.

My point of contact for this action is Mr. William Dates, 275-9483

Miriam F Browning
Director for Information Management

Encl
As

CF: SAAG-PMO-S

Printed on Recycled Paper

Army Materiel Command Comments

DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

REPLY TO ATTENTION OF

AMCIR-A (36-2a) 7 May 1999

MEMORANDUM FOR MR. DONALD C. CRESS, PROGRAM DIRECTOR, ORGANIZATIONAL EFFECTIVENESS, U.S. ARMY AUDIT AGENCY, 3101 PARK CENTER DRIVE, ALEXANDRIA, VA 22302-1596

SUBJECT: DODIG Draft Report, Year 2000 Status of the Army Total Asset Visibility System, Project 9AS-0090 (AMC No. D9925)

1. We are enclosing our position on subject report IAW AR 36-2

2. Point of contact for this action is Mr. Robert Kurzer, (703) 617-9025, e-mail - bkurzer@hqamc.army.mil.

3. AMC -- America's Arsenal for the Brave.

FOR THE COMMANDER:

NORMAN E. WILLIAMS
Major General, USA
Chief of Staff

Encl
as

COMMAND REPLY
DODIG DRAFT REPORT
Year 2000 Status of the
Army Total Asset Visibility System
Project 9AS-0090 (AMC No. D9925)

Finding: Year 2000 Status of the Army Total Asset Visibility System (ATAV)

The USAMC Logistics Support Activity (LOGSA) should not have certified ATAV as Y2K compliant as of Dec 98. The ATAV should not have been certified because supporting test plans and test results showed that LOGSA had tested ATAV in a noncompliant, operating environment and had not performed interface testing. Additionally, the ATAV contingency plan did not adequately provide an overview of the system requirements or discuss the use of manual procedures or testing of the contingency plan itself. Also, LOGSA did not fully distribute and coordinate the contingency plan with the functional users. As a result, without a rigorous system testing and certification process, and a comprehensive contingency plan, the functionality provided by ATAV remains at risk of failure.

Recommendations:

1. We recommend that the Commander, LOGSA:

a. Recertify the ATAV system with the following changes:

Command Comments: Nonconcur. The LOGSA has certified ATAV according to the Department of Defense (DOD) Management Plan.

ATAV is an AMC mission critical system and will be participating in the Army End to End Test (E2ET) beginning 6 May 99 as directed by the SECDEF. Mission critical logistics threads will be tested in conjunction with other Army systems to assure Year 2000 compliance. All mission critical systems must be certified to participate in the E2ET. To require that the Army should "recertify" the ATAV would be impractical and would deny ATAV participation in the OSD sponsored end-to end logistics tests which will start 25 May 99.

In addition, a third party contractor was hired for the ATAV Independent Validation and Verification (IV&V) process

IAW the DOD Year 2000 Management Plan. The contractor has completed this IV&V process and has found ATAV to be certified. To start this process all over again for another certification would put a bill on the table of $34,148. Such a bill is unfunded and for the previously stated reasons would not be considered a prudent expenditure of Army dollars. In summary, the finding does not provide a basis to recertify ATAV.

(1) Discuss the interface testing completed.

Command Comments: The DOD Year 2000 Management Plan was updated to include the following note: "Note for business systems: Certification of interfaces that involve a format change require joint testing by both systems developers. All other interface testing and certification may be conducted independently by the system developer." There was no format change made to ATAV interfaces; therefore, testing was not required.

(2) Require a supporting test plan and results that are dated and signed by the testing official.

Command Comments: Concur. Supporting test plan and results that are dated and signed have been completed.

(3) Complete the certification checklist and note the results of external interface testing completed, rather than responding "not applicable."

Command Comments: Nonconcur. The DOD Year 2000 Management Plan was updated to include the following note: "Note for business systems: Certification of interfaces that involve a format change require joint testing by both systems developers. All other interface testing and certification may be conducted independently by the system developer." There was no format change made to ATAV interfaces; therefore, testing was not required.

b. Write a contingency plan, to be signed and dated by a responsible official, that includes:

(1) A description of the basic interfaces.

Command Comments: Concur. The contingency plan, Version 1.0 dated 16 Apr 99, provides a description of the basic interfaces.

(2) Identification of contingency plan trigger dates, activities, strategies, and procedures to be performed at specified dates or events.

Command Comments: Concur. The contingency plan, Version 1.0 dated 16 Apr 99, includes this information.

(3) A detailed description of manual procedures to be performed.

Command Comments: Concur. Manual procedures and work-arounds have been included in the ATAV contingency plan.

(4) A discussion of the acceptable level of performance and the risk arising from the use of manual procedures.

Command Comments: Concur. Information on acceptable level of performance and risk will be added to the ATAV Contingency Plan NLT 1 Jun 99.

(5) A plan to test the contingency plan itself.

Command Comments: Concur. IAW the DOD Year 2000 Management Plan, the contingency plan for ATAV will be exercised prior to 30 Jun 99.

c. Coordinate the contingency plan with the functional users and all involved with making the plan work and distribute copies of the plan to all interested parties.

Command Comments: Concur. The contingency plan has been coordinated with the functional users and all involved with making the plan work, and copies of the plan will be distributed to all interested parties NLT 30 Jul 99.

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD produced this report.

Thomas F. Gimble
Mary Lu Ugone
Kenneth H. Stavenjord
Kathryn M. Truex
Danny B. Convis
Hugh G. Cherry
Jerry Hall